AMENDMENTS IN THE CLAIMS

1. (currently amended) A method for securely creating an endorsement certificate for a device in an insecure environment, said method comprising:

generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server, wherein the value is a first value that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second value, based on a pre-defined method for determining when to change said first value to said second value from among: a passage of a pre-set amount of device manufacturing time and a preset number of manufactured devices from among the plurality of valid devices, wherein said non-public, secure value is a secret number;

forwarding a first copy of said secret number via a secure communication medium to said credential server;

hashing a second copy of said secret number with a public key from said endorsement key pair;

combining a first hash result from said hashing step with the public key to create the endorsement key (EK);

forwarding said EK to said credential server to initiate a credential process;

verifying by utilizing said non-public, secure value that an endorsement key of said valid device is a valid endorsement key of said endorsement key pair that was generated during manufacture[[d]] of said valid device, wherein a function of a first copy of said non-public, secure value within said credential server matches a similar function of a second copy of said non-public, secure value associated with the endorsement key received at the credential server, said verifying step further comprising:

receiving said EK from said device at the credential server;

hashing the public key within the received EK with the first copy of said secret number received during said forwarding step to provide a second hashed value;

comparing the first hashed value from within the EK with the second hash value; and

confirming said EK is from a valid device when said comparing step results in a match; and

inserting an endorsement certificate into said device to indicate that said device is an approved device by an original equipment manufacturer (OEM) of the device.

2 - 4. (canceled)

5. (original) The method of Claim 1, wherein following said verifying step said method further comprises:

initially storing the credential in a database of said credential server;

monitoring for a request from a customer to provide said certificate to said device; and

following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device.

6. (original) The method of Claim 1, wherein said endorsement certificate is once-writeable public-readable and is utilized for signing said public key during communication from and to said device.

7. (original) The method of Claim 1, wherein said value is injected into said device, and said value is a single-use parameter, said method further comprising immediately destroying said value within said device following a creation of said EK.

8. (original) The method of Claim 1, wherein said credential server is remotely located from a vendor manufacturing said device and said method comprises communicating said value from said device to said credential server via a secure communication medium.

9. (previously canceled)

10. (original) The method of Claim 1, wherein said device is a trusted platform module (TPM).

11. (canceled)

12 - 16. (previously canceled)

17 - 24. (canceled)

25. (previously canceled)